Acronis Cyber Resilience

Ciberresiliencia integrada de forma nativa para servidores y máquinas virtuales

Fortalezca su ciberresiliencia con Acronis

La ciberresiliencia va más allá de la ciberseguridad tradicional. No se trata únicamente de prevenir ataques, sino también de garantizar que las empresas puedan seguir operando incluso cuando se produzcan incidentes. Según la definición del NIST, "la ciberresiliencia es la capacidad de anticiparse, resistir, recuperarse y adaptarse a condiciones adversas, tensiones, ataques o compromisos que afecten a los sistemas".

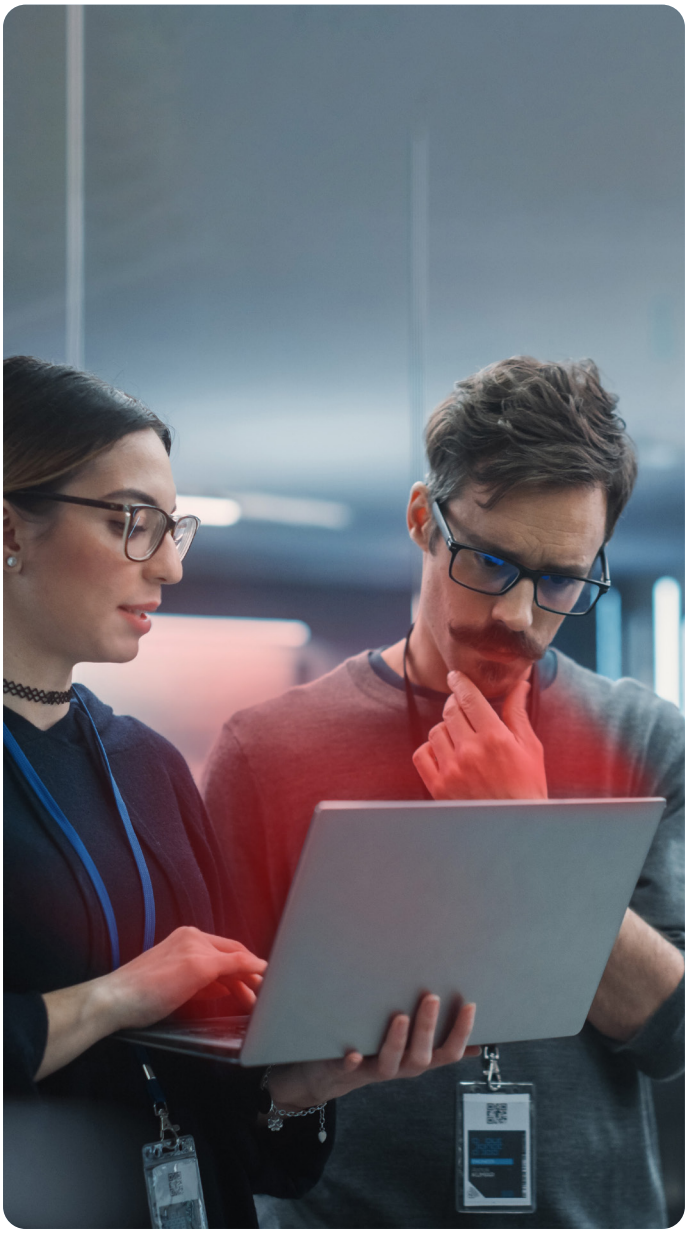
Tanto para los proveedores de servicios como para las empresas, la verdadera pregunta es: ¿cuánto tiempo tardará su negocio en recuperarse tras sufrir un ciberataque? Sin guías tácticas de respuesta ante incidentes, herramientas útiles y objetivos de punto y tiempo de recuperación (RPO y RTO) bien definidos, cada interrupción que se produzca puede conllevar el riesgo de provocar pérdidas de ingresos, disminución de la confianza de los clientes y daños reputacionales duraderos.

Problemas principales de la resiliencia

Todas las empresas, independientemente de su tamaño, están descubriendo que los tiempos de inactividad cuestan mucho más que el hecho de perder datos. Los proveedores de servicios se enfrentan al riesgo añadido de perder a sus clientes, ya que estos cambian rápidamente de proveedor si las interrupciones recurrentes minan su confianza.

Por su parte, las empresas deben afrontar una creciente presión en materia de cumplimiento normativo y supervisión regulatoria. Cualquier deficiencia en la preparación las expone a multas, sanciones y riesgos para su reputación.

La gestión de incidentes con herramientas fragmentadas también propicia una complejidad innecesaria. Sin una estrategia unificada, los equipos de TI experimentan un caos operativo, ya que tienen que lidiar con la detección, la respuesta y la recuperación a través de múltiples consolas y agentes. Estas ineficiencias aumentan los costes, ralentizan los tiempos de respuesta y aumentan la responsabilidad de la empresa.El aumento de las primas de los ciberseguros supone una preocupación adicional, y una resiliencia insuficiente podría incluso traducirse en la denegación total de la cobertura.



Barreras tecnológicas para la resiliencia

A medida que las empresas impulsan su transformación digital, lograr un buen nivel de resiliencia se ha convertido en un desafío aún mayor. Los entornos de TI híbridos abarcan sistemas in situ, plataformas en la nube y endpoints remotos, lo que hace crecer cada vez más la superficie de ataque. Esto da lugar a más interdependencias y a más puntos de fallo únicos. Al mismo tiempo, las amenazas se han vuelto cada vez más sofisticadas. El ransomware, las vulnerabilidades en la cadena de suministro y los riesgos internos están aprovechando las brechas que dejan las soluciones aisladas. Las herramientas individuales pueden reducir ciertos riesgos específicos, pero también generan puntos ciegos, procesos manuales complejos y brechas de seguridad que los atacantes no tardarán en aprovechar.

El camino hacia la ciberresiliencia

Para lograr una verdadera ciberresiliencia se necesita algo más que una protección eficaz. Se trata de garantizar la continuidad operativa, independientemente del tipo de interrupción. Las empresas pueden alcanzar la resiliencia si adoptan un enfoque estructurado que comience por **anticiparse** a los riesgos mediante la asignación de recursos, la evaluación de vulnerabilidades y la administración de parches. A continuación, deben ser capaces de **resistir** las amenazas, al detectarlas y contenerlas en tiempo real mediante funciones avanzadas, como la Detección y respuesta para endpoints (EDR), la Detección y respuesta ampliadas (XDR) y la Prevención de pérdida de datos (DLP). Estas medidas proactivas solo son eficaces si se combinan con una sólida estrategia de recuperación.

La recuperación es el siguiente paso crítico. Restaurar datos y sistemas rápidamente, de forma fiable y sin malware, reduce al mínimo el riesgo de sufrir tiempos de inactividad. En caso de interrupción grave, la máxima prioridad debe ser mantener la continuidad de la actividad empresarial. Con Acronis Cloud Disaster Recovery, las empresas pueden realizar al instante la conmutación por error de las cargas de trabajo afectadas directamente a la nube de Acronis o a Microsoft Azure. Esta conmutación por error inmediata garantiza la continuidad de la actividad empresarial incluso durante las interrupciones más graves, y además actúa como un entorno de respaldo seguro hasta que se complete todo el proceso de restauración de los sistemas principales.

Por último, la resiliencia no es estática. Las organizaciones deben **adaptarse**. Para ello, deben aprender de los incidentes, formar a sus equipos y perfeccionar sus defensas con el tiempo.

El espectro de la recuperación ante desastres

En última instancia, estas estrategias no solo se centran en la recuperación tras un desastre, sino en la resiliencia operativa necesaria para mantener las funciones empresariales esenciales frente a cualquier adversidad. La capacidad de recuperar los servicios en cuestión de minutos, en lugar de días, es la clave para minimizar las pérdidas económicas y mantener la confianza de los clientes.

Las estrategias de recuperación ante desastres se suelen clasificar en función de los RPO y RTO que pueden alcanzar. Dos de las estrategias más adoptadas son las siguientes:

DR nivel intermedio

Este enfoque ofrece un equilibrio entre coste y velocidad de recuperación. Utiliza sistemas preconfigurados que pueden activarse rápidamente, lo que se alinea con el objetivo de "recuperación" al minimizar el tiempo de inactividad, a la vez que mantiene un RPO y un RTO bien definidos.

DR nivel básico

Este enfoque se centra exclusivamente en la reconstitución y la restauración de datos, y se basa en la recuperación completa a partir de las copias de seguridad, lo que da lugar a tiempos de recuperación más largos, pero a costes operativos más bajos.

Al unificar la detección, la protección y la recuperación, las empresas obtienen una ventaja crítica: no solo pueden sobrevivir a una crisis, sino también salir reforzadas de ella. Gracias a Acronis Cloud Disaster Recovery, las organizaciones pueden seleccionar el nivel de resiliencia adecuado para cada carga de trabajo, desde opciones de conmutación por error de nivel intermedio o básico, que permitan recuperar los servicios tras sufrir una interrupción, hasta continuidad casi instantánea con recuperación ante desastres de nivel avanzado. Esta flexibilidad refuerza las defensas en cada etapa del camino hacia la ciberresiliencia.

La solución Acronis Cyber Resilience

Además de la recuperación ante desastres, Acronis proporciona una plataforma integrada de forma nativa que unifica las funciones de copia de seguridad, recuperación ante desastres, seguridad de endpoints, evaluación de riesgos y prevención de pérdida de datos. Este enfoque elimina la necesidad de trabajar con varias soluciones aisladas, reduce la fragmentación de herramientas y garantiza la resiliencia sin añadir complejidad. Diseñada tanto para empresas como para proveedores de servicios, la plataforma cubre todas las etapas del camino hacia la resiliencia: anticipación, resistencia, recuperación y adaptación. Con una sola plataforma, un solo agente y una sola consola, las empresas pueden detectar las amenazas con mayor rapidez, recuperar las operaciones sin interrupciones y adaptarse continuamente a los riesgos en constante evolución.

ANTICIPACIÓN	RESISTENCIA	RECUPERACIÓN	ADAPTACIÓN
• Descubrimiento de dispositivos • Mapa de protección de datos • Inventario de recursos • Evaluación de vulnerabilidades • Administración de parches	• Detección de amenazas en tiempo real • Detección y respuesta para endpoints (EDR) • Detección y respuesta ampliadas (XDR) • Prevención de pérdida de datos (DLP) • Contención rápida de las amenazas activas	• Recuperación de datos segura y automatizada • Recuperación ante desastres en la nube (CDR) • Copias de seguridad inmutables • Movilidad entre hipervisores • Recuperación a puntos libres de malware	• Supervisión y administración remotas (RMM). • Formación de concienciación sobre seguridad (SAT) • Detección y respuesta gestionadas (MDR) • Plantillas guiadas de respuesta ante incidentes

¿Por qué las empresas eligen Acronis?

Para los proveedores de servicios, Acronis ofrece una vía para acelerar la generación de ingresos recurrentes. Al añadir servicios de ciberresiliencia con alto margen de beneficio a su cartera, los MSP no solo amplían su oferta, sino que también logran destacar en un mercado cada vez más competitivo y poco diferenciado. La plataforma unificada simplifica las operaciones al reducir la fragmentación de herramientas, mientras que un modelo de licencia sencillo maximiza los márgenes y se adapta a la perfección a las necesidades crecientes de cada cliente.

Para las empresas y pymes, Acronis garantiza la continuidad de la actividad empresarial gracias a la recuperación rápida y sin malware, que minimiza el tiempo de inactividad y las pérdidas económicas. Las funciones integradas de generación de informes y soporte de cumplimiento normativo facilitan la gestión de auditorías regulatorias. Las funciones eficaces de resiliencia también mejoran la elegibilidad para el ciberseguro, lo que a menudo reduce las primas. Por último, y no por ello menos importante, demostrar una sólida estrategia de resiliencia genera confianza entre clientes, partners y organismos reguladores.

Solicite una reunión con un experto de Acronis

La continuidad de su actividad empresarial depende de algo más que de la protección. Requiere resiliencia. Descubra cómo Acronis puede ayudarle a anticiparse a las amenazas, resistir los ataques, recuperarse más rápido de sus consecuencias y adaptarse de cara al futuro.

CONTÁCTENOS

Acronis

Obtenga más información en www.acronis.com